MAILsweeper™
for SMTP Version 4.2

Manage the content of incoming and outgoing e-mail at the SMTP gateway

e-mail

MIMEsweeper™
policy-based content security

MAILsweeper- Policy-based content security for e-mail

MAILsweeper is the SMTP gateway product from the market leading MIMEsweeper family of content security solutions – the core of your company's system defenses.

Analyzing incoming and outgoing e-mail at the Internet gateway, MAILsweeper enables organizations to implement security policies to detect, block or quarantine inappropriate or threatening e-mails and attachments.

Threats are not always obvious

Threats hidden in the content of e-mail can paralyze your network and devastate your business. Protecting yourself from the consequences of these threats means having a detailed content security policy in place, and a comprehensive system of enforcing it.

The first step is to establish a security policy outlining what is acceptable and what is not. Step 2 is to educate employees on that security policy. Step 3 is to implement a comprehensive solution that is flexible and scalable enough to enforce a constantly changing and evolving policy – MAILsweeper. Your content security solution needs to protect your organization from e-mail threats that can lead to:

- Lost productivity and damage to reputation through e-mail misuse
- Infection and data loss from e-mail-borne viruses
- Confidentiality breaches
- Exposure to legal liability

- Copyright infringement
- Spoof and denial of service attacks
- Network downtime
- Harassment of employees

Organizations are legally responsible for the content on their systems

Without control over the data that enters and leaves the network, companies are prey to a host of security threats. Because every organization is legally responsible for the content on their systems, in the worst cases IT misuse can ultimately end in legal proceedings. High profile instances of this over the years have included:

Network downtime...
Sircam virus infects over 2,300,000 machines causing an estimated $1 billion in damage and network downtime.
– Information Week Sept 2001

Breaches of confidentiality...
Microsoft security compromised...infiltrator believed to have entered via e-mail.
– CNET.com

Loss of productivity...
IDC estimates that the cost in lost productivity incurred by an employer with 1,000 employees could be as much as $96,000 per year.
– IDC Corporation

Damage to reputation...
DOW Chemical sacks workers for circulating pornography by e-mail.
– Computerworld

Legal liability...
Chevron Corp. pays $2.2 million to settle sexual harassment claims. Several female employees said that they had received hostile e-mail, which even included violent pornography.
– Business Today

Data corruption...
The costs of virus and worm attacks on information systems worldwide in 2000 caused business damages totalling an estimated $17.1bn.
– Mummert & Partner

Attention: CEOs, CFOs, CIOs and Legal/Marketing/Sales/HR Directors

- Prevent confidentiality breaches and loss of intellectual property
- Manage legal liability
- Protect against the misuse of e-mail that leads to lost productivity, employee harassment and damage to corporate reputation
- Defend against junk e-mail, spam and spoof attacks

Attention: IT and Network Administration Managers

- Protect against loss of network service through misuse and hostile attacks, such as denial of service
- Reduce network congestion by managing file size and removing attachments
- Manage undesirable file types such as MP3s, AVIs, MPEGS and executables
- Prevent data siphoning and corruption by stripping HTML scripts and mobile code
- Identify and clean or block viruses in incoming and outgoing e-mail

Download and trial MAILsweeper for free

The simplest way to discover just how effective MIMEsweeper solutions are in helping your organization establish and enforce a content security policy - is to try them for free.

For a free trial of the software, just visit our website at: **http://www.mimesweeper.com/download/**

The MIMEsweeper market leading solutions

MIMEsweeper has consistently represented the forefront of content security technology. With over 10,000 customers covering 10 million users around the world, MIMEsweeper is the world's most popular content security solution, the core of your company's system defenses. Delivering solutions to all potential e-mail, web and Intranet based threats.

E-MAIL

▪ MAILsweeper™ for SMTP

Analyzing incoming and outgoing e-mail at the Internet gateway, MAILsweeper allows organizations to implement security policies to detect, block or quarantine inappropriate or threatening e-mails.

▪ PORNsweeper™
Add-on to MAILsweeper for SMTP

Avoid damage to reputation and exposure to legal liability by intelligently analyzing image attachments for nude or pornographic content. Integrating into the MAILsweeper security service, PORNsweeper's unique algorithms analyze image files to detect and flag embedded and attached pornographic content.

▪ SECRETsweeper™
Add-on to MAILsweeper for SMTP

The full encryption and digital signature add-on to MAILsweeper stops coded secrets, offensive material and viruses from entering and leaving your network in S/MIME encrypted e-mail. This provides a secure communications channel to and from trusted parties.

▪ e-Sweeper™

A hosted/distributed e-mail content security solution that enables ISP/ASPs to provide fully hosted content security services for their customers.

WEB

▪ WEBsweeper™

WEBsweeper provides network protection by barring access to selected categories of websites, and by constantly monitoring web, http and FTP transfers for inappropriate or suspect activity. WEBsweeper enables you to identify, block and clean web transfers.

INTRANET

▪ MAILsweeper™ for Lotus Domino

Providing a content security solution for the Intranet enables organizations to manage threats in Domino Mail and Databases.

▪ MAILsweeper™ for Microsoft Exchange 5.5

MAILsweeper for Microsoft Exchange 5.5 provides optimal e-mail security within your Intranet messaging infrastructure by maintaining user productivity and reducing legal liability as well as protecting network integrity.

▪ MAILsweeper™ for Microsoft Exchange 2000

Provides optimal e-mail security within your Intranet messaging infrastructure within a Microsoft Exchange 2000 environment.

Implementing an e-mail content security solution

The solution

E-mail content security is about defining an employee e-mail usage policy to cover what is and isn't acceptable in e-mail and e-mail attachments - and then monitoring and enforcing the policy using a comprehensive, and expandable, software solution.

MAILsweeper allows organizations to implement and enforce e-mail content security policies, in a simple and effective manner. It enables policies to be defined down to an individual user level, if required, and integrates with enterprise directories (e.g. LDAP) for policies that change as the company does. For example, a company's policy may state that no department has a legitimate reason for receiving messages containing executables other than the IT department; or that every message sent in to or out from technical support should be checked for profanity.

Increasing e-mail traffic volumes

According to IDC, 10 billion e-mails were sent daily in 2000, and by 2005 they predict this will have tripled to 35 billion e-mails a day. *Internet Data Corporation – E-mail Usage Forecast and Analysis, 2000 – 2005*

Recent Ferris research also estimates corporate mailboxes will grow from 260 million in 2001 to 435 million in 2005. *Ferris Research – The Corporate Email Market March 2001*

Policy management

MAILsweeper enables organizations to implement and enforce an e-mail content security policy within the framework of clearly defined guidelines for users. This means that different policies can be applied to different users within an organization.

MAILsweeper achieves this through an intuitive 'Policy Manager' enabling administrators to:

- Define and apply organizational, departmental and user policies easily and consistently
- Amend policies to meet changing business needs for individuals or groups
- Apply the appropriate policy to each object passed through MAILsweeper based on the sender and recipient
- Implement rules through 'Policy Scenarios' – single or multiple security operations are possible, such as detecting/blocking file types, advanced text analysis of document content, detecting/ removing viruses etc
- Dynamically update user lists from LDAP directories
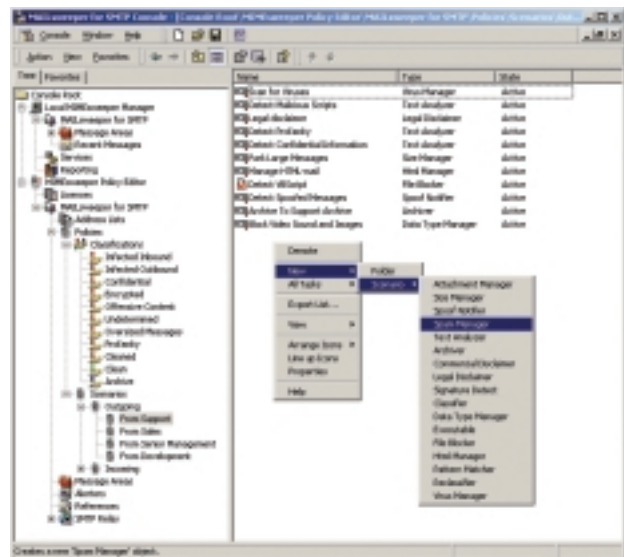
MAILsweeper's simple and powerful policy manager allows rules to be created and amended as new threats arise or policy changes are implemented

Auditing and reporting

MAILsweeper also features comprehensive auditing and reporting functions and includes informative graphical reports to provide detailed information, such as top senders, summary of point-to-point traffic, operational summary and threats detected.

- Up-to-the-minute graphical reporting function
- Auditing to an external MS SQL server database via ODBC
- User-configurable processing views allow you to view data in the way you want
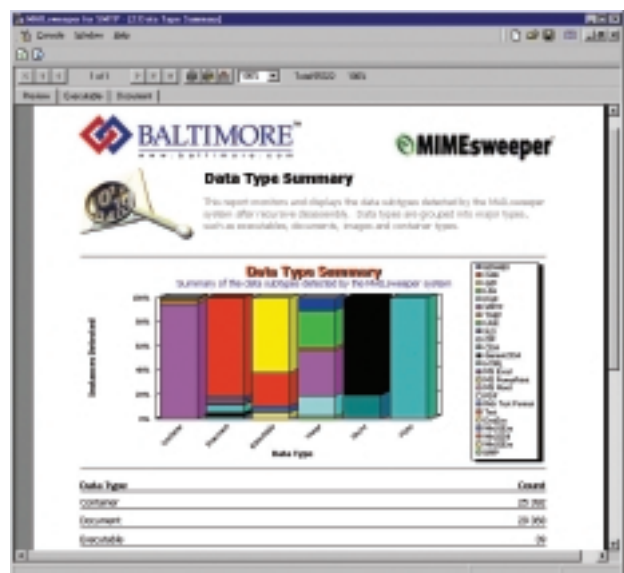
MAILsweeper provides in-depth performance reports and summaries that can be sent to administrators or recipients as defined in the policy

MAILsweeper Defines, Detects and Defends

MAILsweeper is an industry-standard SMTP gateway that analyzes e-mail traffic for content security threats entering and leaving an organization. It disassembles e-mail and e-mail attachments and validates this against the policy, before allowing it to pass, cleaning or detaching any identified threats, or blocking them.

E-mail and attachments are analyzed by MAILsweeper in four stages

Stage 1: Policy identification
Recognition of policy rules as defined by user

- Message sender and recipient determine policy to be applied
- Application of security operation to each message as set up in policy scenarios
- Bi-directional policy application i.e. apply different policies to incoming and outgoing messages separately

Stage 2: Contents disassembly
Recursive disassembly of objects to identify original content

- Recognition and management of key data formats used in e-mail transfers
- Compression/encoding formats – ARJ (including self-extracting ARJ), Gzip, RAR, TAR, PGP, LZH, LHA, CMP, ZIP (multiple variants), BinHex and CAB, MIME, UUE, TNEF and binary
  - Document formats – MS Office (CDA), RTF, HTML, Itchitaro and Fax
  - Executable formats – Windows, DOS, DLLs, Javabyte
  - Image formats – JPEG, DXF, DWG, PSP, DNG, PIC, TIFF, PCX, FIL, BMP and GIF
  - Sound formats – MIDI, AIF, VOL, AU, WAV and MPEG3 (MP3)
  - Video formats – RM, MPEG, GM and AVI
  - Encryption formats – S/MIME (recognized by MAILsweeper for SMTP, scanned with SECRETsweeper), PGP (recognized)
- Detection of custom formats using flexible binary pattern matching
- Recognition of content by file architecture and/or extension
- Detection (or other user-defined actions) of unrecognized data formats

Stage 3: Content Analysis
Analysis of objects according to policy and data type

- Scanning by your choice of industry-known virus scanners including support for multiple virus scanners
- Cleaning and recomposition of infected messages
- Advanced text analysis in message headers, subject line, body text and attachments for keywords, phrases and Boolean expressions including "nearness"
- Customizable detection of data types by binary pattern to detect enterprise-specific content
- Detection and disposal of files by name, size and type
- Conditional actions based on message size and number of attachments
- Attachment of customizable text to e-mails in appropriate character set or US-ASCII e.g. legal disclaimers
- Intelligent analysis of spoofed e-mails
- Detection of inappropriate images (with PORNsweeper)
- Validation of S/MIME signatures and S/MIME encryption or decryption of messages (with SECRETsweeper)

Stage 4: Classification
Selection of disposal path for each message

- Execution of actions e.g. message quarantined, delivered, delayed until user-defined time, copied, returned to sender etc.
- Notification by NT alerts, SNMP traps and e-mail to the administrator

Easy to manage and deploy

As with all products in the MIMEsweeper family, MAILsweeper is easy to manage and provides a robust solution that is scalable and secure.

It can be deployed on the DMZ, as a standalone MAILsweeper host or on the SMTP gateway.
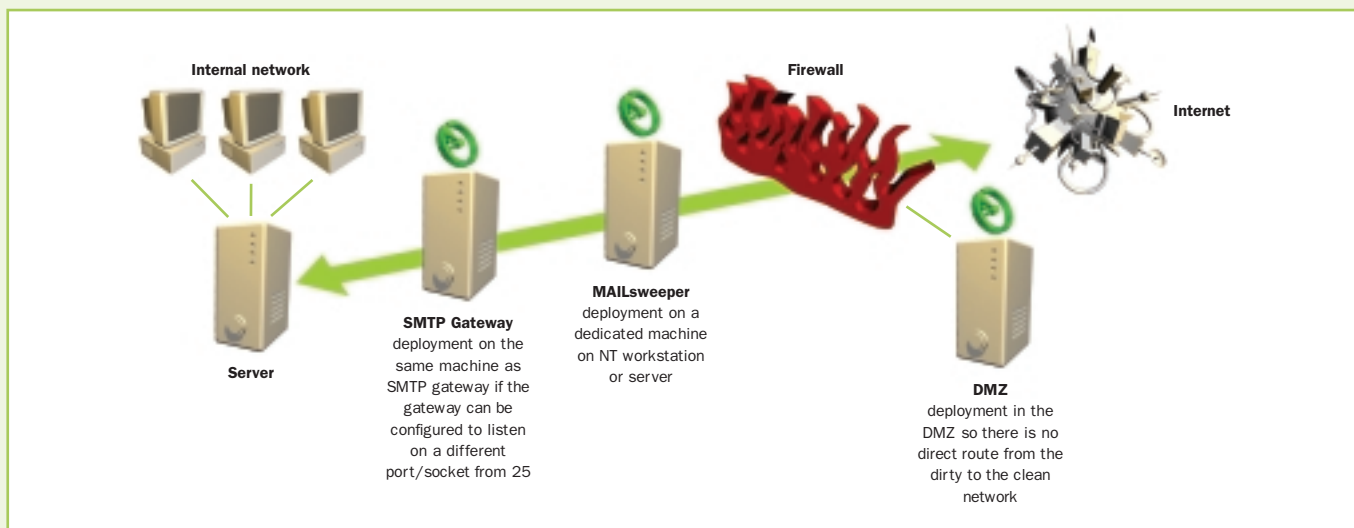
MAILsweeper is a multi-threaded application running on a multi-processor NT 4.0 and Windows 2000-base architecture.

- Increased scalability and resilience achieved through deployment of multiple MAILsweeper servers
- Ease of policy management: implement your policy on one or across multiple MAILsweeper servers
- Ease of system management: real-time statistics on MAILsweeper system performance, as well as managing user use
- Ease of administration: allows remote management via Microsoft Management Console to control services and review message areas and recent message details

- Ease of policy maintenance with LDAP directory integration
- Protect e-mail communication from DOS attacks by controlling the number and duration of incoming SMTP connections
- Powerful reporting: clear operational statistics with user-friendly reporting features
- Secure your site by using anti-relay countermeasures

Technical requirements

- Processor: dependent on configuration and number of uses; minimum recommendation Pentium™ II 400 MHz or equivalent
- 500 MB free space on NTFS partition for installation
- 500 MB free space in /temp directory
- 128 MB memory
- Microsoft Windows™ NT Workstation or Server version 4.0 Service Pack 5 or Windows 2000 Professional or Server with Service Pack 1

- Internet Explorer 5
- Microsoft Management Console 1.2
- Outlook XP for full functionality
- Microsoft Data Access Components 2.1
- TCP/IP networking
- Access to CD-ROM or network for installation
- MS SQL server 7/2000 for reporting

Europe

United Kingdom
1310 Waterside, Arlington
Business Park
Theale
Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 118 903 8000
Fax: +44 118 903 9000

Contact MIMEsweeper:
info@mimesweeper.com

Germany
Amsinckstrasse 67
Poseidonhaus
Hamburg, 20097
GERMANY
Tel: +49 402 399 90
Fax: +49 402 399 9100

Contact MIMEsweeper:
info@mimesweeper.com

France
92 Avenue de Wagram
Paris, 75017
FRANCE
Tel: +33 (0) 1 72 74 63 02
Fax: +33 (0) 1 72 74 63 01

Contact MIMEsweeper:
info@mimesweeper.com

America

USA
1550 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: + 1 425 460 6185

Contact MIMEsweeper:
info@mimesweeper.com

Asia Pacific & Japan

AUSTRALIA
Level 4, Building C
CityWest Office Park
33 Saunders Street
Pyrmont
New South Wales 2009
AUSTRALIA
Tel: +61 2 8514 7300
Fax: +61 2 8514 7301

Contact MIMEsweeper:
info@mimesweeper.com

JAPAN
New Otani Garden Court 8F
4-1, Kioichi-cho
Chiyoda-ku
Tokyo-to, 102-0094
JAPAN
Tel: +81 3 5212 3772
Fax: +81 3 5212 3788

Contact MIMEsweeper:
info@mimesweeper.com

www.mimesweeper.com